*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**
**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**
**http://www.us-cert.gov/tlp/**

**DATE(S) ISSUED:**
09/10/2020

**SUBJECT:**
Multiple Vulnerabilities in Palo Alto PAN-OS Could Allow for Arbitrary Code Execution

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Palo Alto PAN-OS, the most severe of which could allow for arbitrary code execution. PAN-OS is an operating system for Palo Alto Network Appliances. An attacker can exploit this issue by sending a malicious request to the Captive Portal or Multi-Factor Authentication interface. Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated remote attacker to disrupt system processes and potentially execute arbitrary code with root privileges.

**THREAT INTELLIGENCE:**
There is currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**
- All versions of PAN-OS 8.0;
- PAN-OS 8.1 versions earlier than PAN-OS 8.1.15;
- PAN-OS 9.0 versions earlier than PAN-OS 9.0.9;
- PAN-OS 9.1 versions earlier than PAN-OS 9.1.3.

**RISK:**
**Government:**
- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**
- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**
Multiple vulnerabilities have been discovered in Palo Alto PAN-OS, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- Buffer overflow when Captive Portal or Multi-Factor Authentication (MFA) is enabled (CVE-2020-2040)
- Reflected Cross-Site Scripting (XSS) vulnerability in management web interface (CVE-2020-2036)
- Management web interface denial-of-service (DoS) (CVE-2020-2041)
- OS command injection vulnerability in the management web interface (CVE-2020-2037)
- OS command injection vulnerability in the management web interface (CVE-2020-2038)
- Buffer overflow in the management web interface (CVE-2020-2042)
- Management web interface denial-of-service (DoS) through unauthenticated file upload (CVE-2020-2039)
- Passwords may be logged in clear text when using after-change-detail custom syslog field for config logs (CVE-2020-2043)
- Passwords may be logged in clear text while storing operational command (op command) history (CVE-2020-2044)

Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated remote attacker to gain unauthorized access to the affected application.

**RECOMMENDATIONS:**
The following actions should be taken:

- Apply appropriate patches or appropriate mitigations provided by Palo Alto to vulnerable systems immediately after appropriate testing.
- Block external access at the network boundary, unless external parties require service.
- If global access isn't needed, filter access to the affected computer at the network boundary. Restricting access to only trusted computers and networks might greatly reduce the likelihood of a successful exploit.
- To reduce the impact of latent vulnerabilities, always run non administrative software as an unprivileged user with minimal access rights.

**REFERENCES:**
**Palo Alto:**
https://security.paloaltonetworks.com/

**CVE:**
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2036
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2041
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2037
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2038
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2042
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2039
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2043
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2044